



Arcot Fraud Detection and Risk Analysis for eCommerce Transactions

Solution Guide

SOLUTION GUIDE

Overview

Adds an additional layer of protection against fraudulent shoppers.

Analyzes a range of data in the context of each transaction and measures the potential for fraud.

Invisible to legitimate users who engage in behavior that matches their profile and the card issuer's policies.

Cardholder Authentication Programs

In 2000, Visa with help from Arcot Systems defined 3-D Secure, an authentication protocol that allows card issuers to authenticate their cardholders during online transactions.

Visa licensed this technology to MasterCard and JCB to authenticate cardholders in their networks as well, and the programs are known in the marketplace as Verified by Visa, MasterCard SecureCode and JCB J/Secure. The programs all operate in the same way by having cardholders enroll their cards by registering in the program or by the issuer pre-enrolling the cardholder directly in the program. The protocol itself does not define the method of authentication to be used. Most issuers support passwords – the cardholder selects a password as part of the enrollment process. Some issuers support EMV chip card based authentication – notably used with the disconnected reader (MasterCard CAP / Visa DPA). When they shop at participating merchants web sites, registered cardholders must provide this secondary authentication during the “buy transaction”. When used by merchants, some or all of the fraud risk for Card Not Present transactions shifts back to the card issuer. Merchants may also receive a reduced interchange rate for these authenticated transactions.

Enrollment typically requires the cardholder to provide identifying information (date of birth, social security number, address or any other information that was originally provided to the issuer at the time of opening the account) and then establishing a password to be used during purchases.

The card networks have made participation optional for cardholders to balance both issuers' desire to increase participation and merchants' concerns over the effect mandatory participation could have on shoppers abandoning transactions. Some issuers give cardholders the option of enrolling during their online shopping with a participating merchant, in a process known as “Activation During Shopping” or ADS.

Fraud and ADS

Visa and MasterCard require that issuers who want to drive cardholder enrollment through ADS offer an opt-out provision. This provision enables unenrolled cardholders to decline or ‘opt-out’ of enrolling in the program when prompted by an issuer to enroll – in the middle of a shopping transaction. Those cardholders who opt-out of participation may continue to shop. Visa and MasterCard established this requirement based on cardholder surveys and trials that showed considerable cardholder abandonment when they were mandated to enroll. Typically issuers continue to prompt the cardholders to enroll every time they shop. After a certain number of opt-outs (typically 3), many issuers switch to a mandatory enrollment requirement.

Fraudsters take advantage of these opt-out options – they can effectively use a stolen card up to 3 times – opting out each time – and complete the purchase without having to enroll in the program. Current policies in the authentication programs prevent issuers from blocking users who opt-out from enrollment from shopping.

Card Issuer Perspective: Card issuers want to get the cardholders to enroll as quickly as possible in the authentication program and reduce fraud. Many issuers would like to make participation mandatory rather than optional. Issuers have seen other mandatory countermeasures (e.g., activation of card via home phone or using identifying information during activation) reduce the amount of card fraud due to lost, stolen, or counterfeit cards, and they would like to see a similar reduction in online fraud. At the very least, issuers would like to mandate that cardholders with reported fraud be required to enroll.

The issuers are rightfully concerned – since they pick up the liability when they allow a shopper to opt-out and complete the purchase without any authentication. At the same time, other issuers are concerned over potential cardholder inconvenience and annoyance of the repeated prompting of low-risk cardholders to enroll their cards. Some issuers want their best, low-risk cardholders to be prompted just once or not prompted at all.

Merchant Perspective: Merchants want to see cardholders participate in the programs as well so that they can shift the risk of fraud loss to the issuers, but not at the expense of lost business. Merchants are particularly concerned about abandoned transactions – since these represent customers who have committed to buy something and entered their card information before being prompted for authentication or enrollment (ADS). Merchants with a manageably low volume of fraud also feel that making ADS mandatory would apply a one-size-fits-all approach to dealing with fraud. Mandatory ADS would trade one set of problems caused by fraudulent customers with another that would apply to all customers due to abandoned transactions.

Problem: Balancing Security and Convenience While Reducing Fraud

All three groups, card networks, issuers, and merchants face the same dilemma: How to maintain a balance between security and user convenience. All need to reduce risk and provide consumer assurance while making online purchasing simple and cost effective.

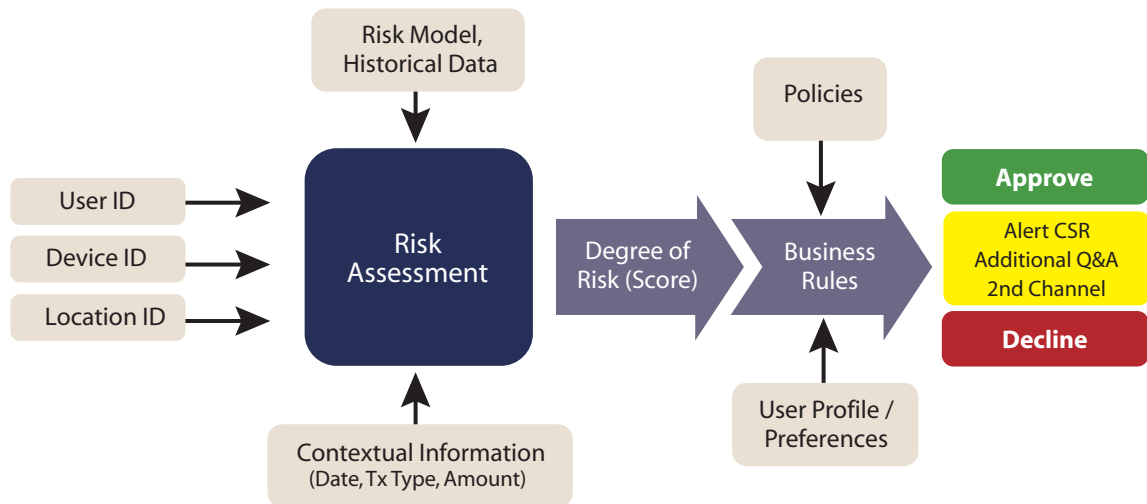
Solution: Risk-based Authentication

Risk-based authentication provides an additional layer of protection for card issuers against fraudulent shoppers who optout of enrolling their cards. This approach is invisible to legitimate cardholders. By analyzing a range of data in the context of each transaction, risk-based authentication identifies the likelihood of potentially fraudulent activity on a transaction by transaction basis. Legitimate users who engage in behavior that both matches their profile and the authentication policies established by the card issuer are allowed to pass unchallenged or are offered an option to enroll with opt-out privileges. Potentially risky users are mandated to authenticate themselves and enroll in the program or are not allowed to complete the purchase.

Risk-based authentication offers two significant benefits:

- 1) Identifies, challenges and potentially blocks the small percentage of fraudulent transactions
- 2) Simplifies the shopping experience for a majority of transactions resulting in increased spending and customer loyalty

FIGURE 1: ARCOT RISKFORT RISK ANALYSIS PROCESS



Arcot RiskFort

Arcot RiskFort is a risk-based authentication application that provides this extra layer of protection against fraud while balancing all of the other factors. It assesses the risk of every transaction, in real time, by examining data collected automatically in the transaction flow. This data includes all the merchant data – the merchant ID, the merchant location and even the merchant category; the transaction data – the transaction amount and transaction currency; and the session data – the IP address of the shopper, the device ID of the shopper and the device type of the shopper. RiskFort compares the current contextual information with historical data and statistical analysis to identify anomalous activity and then calculates a Risk Score for the transaction. Card issuers can use this score to make the best possible business decision based upon all of the factors: Approve or decline the transaction, ask for additional authentication, or alert a customer service representative.

Additionally, RiskFort can adaptively use other tools such as Fair Isaac Falcon to enhance the data-driven decision process.

Key Benefits of RiskFort

- Block Fraud in Real-Time: Reduce fraud before any losses occur by evaluating each transaction as it's occurring
- Invisible to legitimate users: RiskFort only affects risky transactions – most legitimate users will never know it's there

Key Features of RiskFort

- Easy Deployment: RiskFort can be easily added to an existing 3-D Secure deployment and configured for immediate use.
- Configurable policy engine: Easily configure rules to match risk tolerance (e.g., “amount > USD2000 OR amount >GBP1000”) to match rules unique to each issuers environment and policies
- Updatable lists: Easily add to list of positive and negative merchant IDs and IP addressees. Share data with other issuers and benefits from trends observed by other issuers.
- Simple reports: RiskFort marks the risk level of each transaction and the reason for that assessment. Administrators can easily sort these reports and perform “what-if” analysis to reconfigure policy rules to get optimal results.
- Low overheads: RiskFort adds very little overhead in terms of latency to complete its assessment – so cardholders are not held up because of risk assessments.

Balancing Risk Reduction and User Convenience

The success of risk based authentication is determined by three metrics.

Fraud Reduction: Clearly the most important metric is fraud reduction. This is measured by computing the monthly fraud before and after deploying the risk based authentication program. But this is also a very difficult metric to use to tune the system. Fraud is known 30-120 days after a transaction has been authorized. And by then, the pattern of fraud has also changed.

Review Rate: This is the percentage of transactions that are flagged as being potentially risky. A higher review rate potentially leads to higher fraud reduction, but also negatively impacts the customer experience. In general, the review rate should not be more than 2-3 times the fraud rate. So, if an issuer has seen that 1.5% of transactions are fraudulent, not more than 3-5% should be marked as potentially risky.

False Positive Rate: This is the percentage of transactions that are incorrectly flagged as being potentially risky and is related to the Review Rate. The higher the Review Rate, the higher the False Positive Rate. Considering the earlier example, if 1.5% of transactions are fraudulent and 3.5% are flagged as being potentially fraudulent, then at least 2% of the transactions are incorrectly marked as risky.

The Review Rate is a metric that is immediately known and easily usable to tune the system. The exact False Positive Rate can be determined only after true fraud information is available (same 30-120 day window), but a reasonable estimate can be inferred immediately based on whether the user successfully completed the authentication challenge or failed and abandoned the transaction.

Case Study

A top 10 card issuer in the US added RiskFort as an additional layer of fraud prevention as a supplement to its 3-D Secure program. The issuer deployed this solution to cover a small number of BINs in its portfolio. Over a period of 3 months the issuer saw significant reduction in fraud and expanded the solution to cover additional BINs. The issuer later deployed this solution to all BINs and cards in its debit and credit portfolio.

The issuer had rolled out its 3-D Secure program using Arcot's TransFort Hosted Service (THS) and configured the solution for 3 opt-outs during ADS. Over a period of a year, the issuer saw significant fraud, – mostly related to (shoppers who had opted-out when asked to enroll as part of ADS). In particular, the issuer was concerned that some cardholders had multiple fraud charges on their accounts.

Arcot worked with the issuer to develop the risk-based authentication solution for the issuer. After analyzing the fraud that the issuer had seen over the past few months, Arcot deployed RiskFort with specific configurations to combat the issuer's fraud pattern:

- (a) Each ADS transaction (un-enrolled cardholder) was analyzed on the basis of 3 transaction elements – the shopper's IP address, the Merchant ID and the Amount of the transaction. If the transaction originated from a list of known bad IP addresses, or from a list of suspect Merchant IDs or was over a specified amount (different values for different currencies) then it was automatically flagged as suspect.
- (b) Every cardholder who called in to report a fraud was automatically marked for mandatory enrollment the next time the card was used in a 3-D Secure transaction.

Arcot closely monitored both the Review Rate and the Success Metric defined as “% of successful authentications relative to all transactions that are not opt-outs”. This metric was consistently over the required 95%, while the Review Rate stayed below the target 2.5%.

The abandonment rate for this issuer went up by about 1% representing over 50% of the transactions that were flagged as suspect – fraudsters who were shopping abandoned the transaction when faced with mandatory authentication challenges. The issuer randomly polled cardholders to confirm that they had not been affected by the mandatory ADS. The effective False Positive Rate was less than 50%, meaning over half the transactions flagged as suspect were really fraudulent transactions that were prevented.

During the two months reviewed here, the issuer prevented over \$550,000 in fraudulent transactions. These are purchases that did not have to be charged back to merchants, nor taken as losses by the issuer.

This approach focused on a few key elements of the transaction (a subset of the elements that RiskFort can work with). Through a careful analysis of the fraud pattern, the issuer was able to affect significant savings while not impacting the cardholder experience.

About Arcot

Arcot is the cloud authentication leader. Our fraud prevention, strong authentication, and e-Document security solutions make Web transactions and online access safe for millions of consumer, enterprise, and e-Commerce users.

Organizations can transparently deploy stronger authentication and allow users to conveniently authenticate from any computer or mobile device. Arcot solutions deliver the right balance of cost, convenience and strength.

For more information, please visit www.Arcot.com, email sales@arcot.com, or contact your nearest sales office:

Corporate Headquarters, U.S.
Arcot Systems, Inc.
Ph: +1 408 969 6100

United Kingdom
Arcot International
Ph: +44 118 965 7998

Germany
Arcot Deutschland GmbH
Ph: +49 8157 997793

India
Arcot R&D Software Private Ltd
Ph: +91 80 6660 2745



www.arcot.com

Copyright © 2010 Arcot Systems, Inc. All rights reserved. Arcot, Arcot WebFort and ArcotID are registered trademarks of Arcot Systems, Inc. All other trademarks are the property of Arcot Systems, Inc. or their respective owners.

10-84